WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN 312836)
jdanderson@willkie.com
DAVID D. DOAK (SBN 301319)
ddoak@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
NADIM HOUSSAIN (SBN 335556)
nhoussain@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC-SVK
(Consol. w/ 3:32-cv-02343-VC)

DEFENDANT GOOGLE LLC'S MOTION TO DISMISS SECOND AMENDED COMPLAINT

Date: November 7, 2024
Time: 10:00 a.m.
Ctrm: 4 – 17th Floor (San Francisco)
Before: District Judge Vince Chhabria

Consol. Complaint Filed: July 13, 2023
SAC filed: August 12, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules & Other Authorities

NOTICE OF MOTION

TO ALL ATTORNEYS OF RECORD: PLEASE TAKE NOTICE that the following Motion will be heard on November 7, 2024, at 10:00 a.m., in Courtroom 4, 17th Floor, of the United States District Court for the Northern District of California, located at 450 Golden Gate Avenue, San Francisco, California 94102, with the Honorable Vince Chhabria presiding.

Defendant Google LLC ("Google") does move the Court pursuant to Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the Second Amended Consolidated Class Action Complaint ("SAC") with prejudice because any amendment of the SAC would be futile. The Motion is based on this Notice of Motion and Motion, Memorandum of Points and Authorities, concurrently filed Request for Judicial Notice ("RJN"), Declaration of Nadim Houssain in Support of the RJN and attached exhibits, all pleadings and other papers on file in this action, and any other evidence or argument that may be presented to the Court in connection with this Motion.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

After six complaints[1] totaling several hundred pages, Plaintiffs still can't plausibly allege misconduct. It's now time to dismiss the complaint with prejudice.

This case, now over a year old, already went through an unsuccessful motion for preliminary injunction. Plaintiffs prepared expert reports, including one the Court excluded on reply because it wasn't submitted with the motion. Google demonstrated the falsity of Plaintiffs' allegations then. Following the Court's denial of the motion for preliminary injunction, Plaintiffs amended, and the Court found that, even applying the pleading standard, the complaint was implausible. Plaintiffs have now amended yet again, but after six attempts, there is simply no reason why Plaintiffs should not be able to allege the facts necessary for their claims to survive, *other than* that they don't exist. No Plaintiffs suffered any harm—no instances of targeted

[1] *See* Jane Doe v. Google LLC, No. 5:23-cv-02343 (N.D. Cal. 2023), Dkt. 1 (Class Action Complaint); *John Doe et al. v. Google LLC*, No. 3:23-cv-02431-VC (N.D. Cal.), Dkt. 1 (Class Action Complaint), Dkt. 16 (Amended Class Action Complaint), Dkt. 41 (Consolidated Class Action Complaint), Dkt. 86 (FAC), Dkt. 158 (SAC).

advertising, no violation of privacy, no tracking, nothing. If they had, it would be somewhere in the 107 pages that now make up the SAC.

Nor could Plaintiffs allege that anyone else has suffered harm. Indeed, facing the reality that Google did the right thing and classified these websites in a manner that prevents them and Google from engaging in inappropriate targeting, Plaintiffs now pivot to a new avalanche of supposed uses to which Google has allegedly put the websites' data. Just like their last accusations, all these new supposed uses are lifted straight from Google's Help Pages. But anyone can read those pages and conjure a claim based on speculation. Rule 8 requires more. Rule 9(b), far more.

More offensive still is that Plaintiffs accuse Google and healthcare companies of conspiring to engage in a massive fraud on the public and a campaign to invade user privacy, all supposedly to capture private health information to serve better ads (never mind that Plaintiffs already learned at the preliminary injunction stage that this isn't happening). These accusations are baseless. They trigger Rule 9(b) for good reason, and Plaintiffs cannot meet that bar.

In dismissing the last complaint, this Court identified multiple deficiencies with Plaintiffs' complaint: the self-contradictory nature of Plaintiff's allegations, the fact that the most important allegations were conclusory and lacked specificity and plausibility, not to mention the length and number of exhibits attached. Dkt. 157. The SAC fails to cure these deficiencies. It's time to put this to bed. Google respectfully asks the Court to dismiss with prejudice.

II. STATEMENT OF ISSUES

Whether the SAC should be dismissed for failure to state a claim upon which relief can be granted under Federal Rule of Civil Procedure 12(b)(6), and whether the claims should be dismissed with prejudice where amendment would be futile.

III. BACKGROUND

A. Plaintiffs' new complaint fails to plead specific facts to support their claims, and similar cases against healthcare providers are ongoing or have failed.

Plaintiffs, proceeding anonymously, are seven patients of six healthcare providers—Gundersen Health System, Kaiser Permanente, Tallahassee Memorial Health Care, MedStar

Health, Shannon Medical Center, and Edward-Elmhurst Health—and brought this lawsuit against Google arising from their interactions with their healthcare providers' websites (the "Websites"). SAC ¶¶ 35–81. Plaintiffs purport to represent a class of all persons in the United States whose "Health Information was obtained by Google through Google Source Code from their Health Care Provider" and a subclass of Google account holders. *Id.* ¶ 191. The SAC purports to cover healthcare providers' use of four Google products—Google Analytics, Google Ads, Google Tag, and Google Tag Manager—on their websites and apps. *Id.* ¶¶ 25–29. However, the Websites are alleged to utilize only two Google products—Google Analytics and Google Ads. *Id.* ¶¶ 35–78.

Plaintiffs claim that, on various dates, they visited the Websites to search for medical professionals, pay bills, schedule appointments, view medical records, medications, test results, and communicate with doctors. *Id.* Plaintiffs claim the Websites placed Google Ads and Google Analytics source code on specific pages of the Websites. *Id.* Plaintiffs claim that data could have been transmitted through those interactions, and that such data included URLs, "events" and "parameters," IP address, user agent, cookies, and device properties. *Id.* ¶¶ 82–101. Plaintiffs claim that some set of information regarding their visits to the Websites was transmitted to Google without their consent, that such information constitutes Health Information, and that Google knew and intended to receive the Health Information. *Id.*; *see also id.* ¶¶ 145–73.

Plaintiffs assert that Google used the data it received from the Websites for advertising purposes, including AI models, conversion tracking, and ad placements; to develop new products and services; and to personalize content. *Id.* ¶¶ 123–44. Plaintiffs do not claim they received any targeted ads or personalized content from Google based on their interactions with the Websites.

Though only Google has been named as a defendant here, there have been other lawsuits brought against at least five of the six Websites (as well as other healthcare providers mentioned in the SAC) in federal and state courts across the country. *See, e.g.*, *John Doe v. Gundersen Health Sys.*, Case No. 2023CV000409 (Cir. Ct. La Crosse Cnty.) ("*Gundersen Health System*"); *John Doe et al. v. Kaiser Found. Health Plan, Inc.*, Case No. 23-cv-02865-EMC (N.D. Cal.); *John Doe I and Jane Doe I v. MedStar Health, Inc. et al.*, Case No. 1:23-cv-01198-JMC (D. Md.) ("*Medstar I*");

John Doe II et al. v. MedStar Health, Inc. et al., Case No. 24-C-20-000591 (Cir. Ct., Baltimore Cnty.) ("*Medstar II*"), *Stein et al. v. Edward Elmhurst Health*, Case No. 1:23-cv-14515 (N.D. Ill.); *D.S. v. Tallahassee Mem'l Healthcare*, Case No. 4:23-cv-00540-MW-MAF (N.D. Fl.). In some cases, the lawsuits are ongoing; in others, the lawsuits have been dismissed. *See, e.g.*, *MedStar II* (July 9, 2024) (granting MedStar's motion for summary judgment where plaintiffs alleged MedStar transmitted health information to Google through the MedStar patient portal).

Some of these lawsuits were brought by the same Plaintiffs' counsel that represent Plaintiffs in this case, and assert claims based on the same or similar facts. *See, e.g.*, *Gundersen Health System*, *MedStar Health I; MedStar Health II*. However, because the plaintiffs in many of the healthcare provider lawsuits have chosen to proceed anonymously, Google is unable to determine whether issue or claim preclusion might apply to any of the claims asserted in the SAC. Plaintiffs' counsel have an obligation to the Court to avoid inconsistent factual allegations made and legal positions taken by each plaintiff, although neither the Court nor Google is able to assess the consistency of those allegations because of counsel's use of *Doe* plaintiffs.

B. Plaintiffs have had six opportunities to plead a viable case.

Plaintiffs Jane Doe, et al., filed an action against Google in *Jane Doe, et al. v. Google LLC*, No. 5:23-cv-02343 (N.D. Cal.) on May 12, 2023. Plaintiffs John Doe I, et al., filed the instant case on May 17, 2023. Dkt. 1. The Court consolidated the cases on June 30, 2023. Dkt. 35. On July 13, 2023, Plaintiffs filed a motion for preliminary injunction, requesting that the Court enjoin Google from allowing approximately 6,000 healthcare provider websites from using Google ads and analytics products. Dkt. 42. The Court denied Plaintiffs' motion on October 18, 2023. Dkt. 76.

Twelve individual plaintiffs filed a 188-page First Amended Consolidated Class Action Complaint ("FAC") on November 16, 2023, asserting 12 claims. Dkt. 86. Google moved to dismiss the FAC on December 21, 2023. Dkt. 88. A hearing was held on March 14, 2024. Dkt. 119. The Court issued an order on May 31, 2024, stating it is "tentatively inclined to dismiss the entire complaint with leave to amend," but allowed Plaintiffs to file a supplemental brief. Dkt. 145 at 1.

Plaintiffs filed a supplemental brief on June 7, 2024 (Dkt. 146), and following invitation of the Court (Dkt. 151), Google filed a response on June 25, 2024 (Dkt. 152).

The Court issued an Order Granting Motion to Dismiss on July 22, 2024, wherein the Court dismissed the FAC in its entirety. Dkt. 157. In its Order, the Court stated that "[i]t would be reasonable, considering the number of chances the plaintiffs have already been given, to dismiss the complaint with prejudice." *Id.* at 20–21. However, the Court ultimately allowed Plaintiffs "one last chance" to amend, but warned Plaintiffs that "if the next iteration of the complaint is remotely close to 188 pages, the plaintiffs will only be hurting their chances." *Id.* at 21.

Seven individual plaintiffs filed a 107-page SAC on August 12, 2024, asserting seven claims against Google: Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.* ("Wiretap Act") (Count 1); California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.* ("CIPA") (Count 2); Invasion of Privacy, Cal. Const. art. I, § 1 (Count 3), Intrusion Upon Seclusion (Count 4); Breach of Contract (Count 5); Breach of Good Faith and Fair Dealing (Count 6); and Unjust Enrichment (Count 7). Dkt. 158. Google now moves to dismiss the SAC with prejudice.

IV. LEGAL STANDARD

The Court is familiar with the legal standard on a motion to dismiss. In addition, Google stresses here that "when a complaint is needlessly long and contains largely irrelevant, distracting, or redundant information, dismissal under Rule 8(a) is appropriate." *Cousart v. OpenAI LP*, 2024 WL 3282522, at *1 (N.D. Cal. May 24, 2024) (citation omitted).

Further, the heightened pleading requirements of Rule 9(b) extend not just to claims of fraud, but to allegations of fact that necessarily constitute fraud. Fed. R. Civ. P. 9(b); *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009). Plaintiffs must allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (quotations omitted); *see also Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

Finally, denial of leave to amend is justified when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *See Carvalho v. Equifax Info. Servs., LLC*, 629

F.3d 876, 892 (9th Cir. 2010). A "district court's decision to deny leave to amend is particularly broad where plaintiff has previously amended the complaint." *Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1058 (9th Cir. 2011) (quotation marks omitted).

V. ARGUMENT

A. Plaintiffs' SAC demonstrates they never had a basis to file this case.

In its Order Granting Motion to Dismiss, this Court found "three overarching problems with the complaint that affect the outcome for most of the claims": (i) lack of specificity regarding Plaintiffs' alleged "investigation" and allegations; (ii) generic product descriptions; and (iii) lack of intent. Dkt. 157 at 4–10. Each overarching problem remains.

1. Plaintiffs' "investigation" remains nothing more than speculation.

Like the FAC, Plaintiffs' SAC is replete with baseless accusations of fraud and conspiracy. *See, e.g.*, SAC ¶¶ 97–98 ("Google's disguised third-party cookies"), 256 ("Google conspired with Health Care Providers"), 265–70 (Google "disguised" first-party "ghost cookies" as "third-party cookies"), 153 (describing Google's HIPAA policy as "self-serving"), 155 (claiming Google's terms and policies "downplayed and obscured the risks"), 158 (claiming that Google misleadingly assures customers that "identifiability is within [their] control"), 159 (claiming that the truth was "contrary to the impression that Google sought to provide in its marketing materials"), 162 (describing Google's HIPAA policy as "farcical"). But, in two astonishing admissions, Plaintiffs demonstrate their fundamental lack of understanding of the Rule 8 and 9(b) standards. First, they claim that any misconduct Google has not publicly denied is misconduct the Court can safely assume Google engaged in. *See* SAC ¶ 171 ("To the extent Google claims to take any action to protect privacy in such information at all, Google only claims to exclude the information from being used in some, not all, of Google's advertising products and services."). And they argue that, to the extent they cannot allege with a good faith basis that a particular product violated their privacy, they nevertheless ask the Court to keep the product in the case. *See id.* ¶ 79 ("[T]o the extent Plaintiffs do not present evidence regarding transmissions involving additional subdomains herein, they do not allege that such transmissions did not, in fact occur.").

Defendants are not required to deny all possible misconduct to be free of accusations of fraud and criminal activity, and the absence of factual allegations cannot form the basis of allegations in a complaint under Rule 8, let alone Rule 9(b). Plaintiffs have turned the way this works on its head, even in the wake of the Court's Order explaining more was required.

Indeed, Plaintiffs make only one attempt to satisfy the "who, what, when, where, why, and how" requirements of Rule 9(b). *See* SAC ¶ 98 (alleging the "who" is Google and its engineers and the rest is, pretty much, "everything, everywhere"); *Vess*, 317 F.3d at 1106. This one attempt falls woefully short of pleading each requirement with particularity, failing to identify, *inter alia*, any statement or disclosure where Google misrepresented the true nature of the cookies at issue, or when or where the alleged misrepresentation occurred. *See Vess*, 317 F.3d at 1106–07 (plaintiff failed to satisfy Rule 9(b) where he did not "identify any specific misrepresentations or specify when and where they occurred."). And the rest of the allegations the Court identified as insufficiently specific remain as vague as they were in the FAC.

a. Plaintiffs still fail to identify all of the locations where the allegedly problematic source code is placed.

The Court stated that Plaintiffs' FAC and exhibits "leave the reader conspicuously unable to discern whether the source code is placed on web pages where it doesn't belong, and if so, how commonly this happens." Dkt. 157 at 6. While the SAC now includes a few URLs wherein "Ads Code," Doubleclick Ads Code," and "Analytics Code" was allegedly present, the SAC does not specify whether those pages are authenticated or unauthenticated, or how commonly the code is found. *See* SAC ¶¶ 40, 48, 57, 62, 70, 76. This is significant because the use of "tracking technology" on an unauthenticated healthcare-related webpage, even where an IP address is transmitted in connection with a visit to that page, does not constitute individually identifiable health information ("IIHI") under HIPAA. *See Am. Hosp. Ass'n v. Becerra*, 2024 WL 3075865, at *14 (N.D. Tex. June 20, 2024); RJN Ex. 10. Some of the URLs are ostensibly login pages (based on the URLs, though Plaintiffs do not allege it for sure), but those do not constitute "user-

authenticated webpages," either. *See* RJN Ex. 10 at 5 (describing "user-authenticated webpages" as webpages that "require a user to log in before they are able to access the webpage").

Plaintiffs pointedly do *not* allege that *any* of the listed URLs are accessible only *after* logging into a patient portal. *See* SAC ¶¶ 40, 48, 57, 62, 70, 76. Plaintiffs claim that, "[a]s a general rule, when Google Source Code appears on a single page of a web property, it also appears on *every* other page of that web property." *Id.* ¶ 114. However, this claim is nothing more than naked generalized speculation that does not deserve the assumption of truth. It is also contradicted by Plaintiffs' own allegations: the lists of specific URLs they allege contain source code clearly do not include every page of that Website, nor do they allege that any of the listed URLs are in fact authenticated pages accessible only after a login. *See* SAC ¶¶ 40, 48, 57, 62, 70, 76.

And, even if an authenticated page did contain source code, that does not mean that the data transmitted from that page necessarily constitutes IIHI or protected health information ("PHI"). Rather, "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care." See RJN Ex. 10 at 4–5.

b. Plaintiffs still fail to precisely describe the type of information that is allegedly transmitted.

The Court noted that Plaintiffs "fail[] to use precise language when describing the type of information that is allegedly transmitted." Dkt. 157 at 5. The SAC still fails to identify what data of Plaintiffs, if any, was transmitted to Google. Though Plaintiffs claim that Google source code was present on the URLs listed in the SAC, it is unclear from the SAC which, if any, of those URLs Plaintiffs actually visited. For example, John Doe I alleges that "Ads Code" was present on www.gundersenhealth.org/services/pregnancy-birth/before-baby-preparing-for-pregnancy, but does not allege that he ever visited that URL, or that he did so because of any reason related to his

health care, rather than for purely informational purposes (analytics and ads code on educational pages do not present any of the alleged issues raised by Plaintiffs' claims). SAC ¶¶ 38–40.

Another example: the SAC provides an "example" of data that is allegedly intercepted when booking an appointment with urologist Dr. Joseph Endrizzi, but no plaintiff alleges that they ever booked an appointment with Dr. Endrizzi. SAC ¶ 89. Though Plaintiffs attach Exhibits 1 and 2, conclusively describing them as "content" and "intercepted communications," the exhibits are merely hypothetical examples of transmissions—they do not show what data would have been sent through the actions Plaintiffs actually took on the Websites, since they do not contain Plaintiffs' specific searches or communications with their specific doctors.[2] *Compare* Dkts. 158-1 and 158-2, *with* SAC ¶¶ 38, 45–46, 60, 74. And, though Plaintiffs claim that the Websites transmitted IP address, no IP address is depicted in the exhibits. *See* SAC ¶ 92; Dkt. 158-1; Dkt. 158-2. Nor is the transmission of IP address alone actionable. *See infra* Section V.B.3–4.

As for Plaintiffs John Doe V and Jane Doe VI, they allege only that Google code was present on the Websites they visited, but do not include any examples of allegedly intercepted communications relating to their healthcare providers (TMH and Shannon Health). *See id.* ¶¶ 56–57, 69–70; Dkt. 158-1. And, of course, none of this can form the basis of a competent allegation that Google used the information, as opposed to merely stored it for the use of the Website that collected it (which has its own relationship and contractual terms with its users).

[2] Exhibits 1 and 2 are also improper under Federal Rule of Civil Procedure 10(c) because they appear to be taken from expert-generated reports. *Compare* Dkts. 158-1 and 158-2, *with* Dkt. 42-1 (Declaration of Richard M. Smith); *Yuan v. Facebook, Inc.*, 2021 WL 4503105, at *2 (N.D. Cal. Sept. 30, 2021) (holding that expert reports generated for litigation are not "written instruments" under Rule 10(c)). The exhibits are also of questionable origin, reliability, accuracy, and value, and are provided with little to no context. The SAC does not explain: who generated the documents; what types of data are actually transmitted to and stored by Google versus dropped upon arrival (like IP address in Google Analytics 4, *infra* Section V.B.1); or which pieces of otherwise inscrutable information they claim are personally identifiable. Exhibits 1 and 2 are also not subject to judicial notice, as they contain facts that are subject to reasonable dispute and cannot accurately and reliably be determined. See Fed. R. Evid. 201(b). The exhibits, at most, demonstrate that some webpages have cookies on them; they are good for nothing else.

c. Plaintiffs' SAC fails to include any specific allegations regarding apps, Google tag, or Google Tag Manager.

Plaintiffs' SAC lacks any allegations relating to "apps," Google Tag, or Google Tag Manager. *See* SAC ¶¶ 2, 21, 23–32, 191. Plaintiffs allege they used six Websites, and that those Websites used only two out of the four accused Google products—Google Ads and Google Analytics. Plaintiffs do not allege they used any healthcare provider *apps*, or allege facts regarding Google's code, how it operates, and what data (if any) is transmitted from apps.[3] Plaintiffs' SAC, at most, encompasses only six Websites that use Google Ads and Google Analytics.

2. Plaintiffs' regurgitation of the Google Help Center remains generic.

Plaintiffs *still* do not allege that they ever saw a targeted advertisement (or any ad at all) related to their health after interacting with the Websites.[4] Perhaps recognizing this deficiency, the SAC advances alternative theories—that even if no health data was used for targeted advertising, Google could have used health data to (1) "classify" individuals, web properties, and Internet browsing activities; (2) inform other ads-related products, such as ads bidding, placement targeting, Performance Max/artificial intelligence, conversion tracking; (3) develop new products and services; or (4) "personalize content." SAC ¶¶ 123–44.

As for category (1), Plaintiffs claim that Google categorizes the data transmitted from each Website, but the only basis they cite for this claim is a webpage that does not support that conclusion. SAC ¶ 127 n.45. The webpage pertains to the Google Ads API, and lists "verticals for targeting or excluding categories of placements," with no explanation as to whether the categories apply to websites, apps, individuals, or how they are assigned. *Id.* Plaintiffs do not mention the Google Ads API anywhere else in the SAC or allege that any of the Websites used the API.

[3] In another case pending before this District, Plaintiffs' counsel conceded that the allegations in this case do not focus on apps, but rather on websites. Plaintiffs' Opposition to Google LLC's Statement of Recent Decision at 1, *Frasco et al. v. Flo Health, et al.*, No. 3:21-cv-00757-JD, (N.D. Cal. Aug. 12, 2024), Dkt. 472 ("The *Doe v. Google* case primarily concerns allegations regarding Google source code underlying various *websites*.") (emphasis added).

[4] Plaintiffs assert that Google, despite stating that it prohibits sensitive interest category advertisers from using advertiser-curated audiences, does not enforce the policy, and as a result, some healthcare providers are still able to use advertiser-curated audiences. SAC ¶¶ 133–35. Plaintiffs again fail to provide any support for these conclusory allegations.

Plaintiffs then claim that Google uses the categories to create "segments" of visitors based on their interactions with the Websites, including "affinity" segments. *Id.* ¶ 128. But this allegation is directly contradicted by another webpage they cite, which provides a representative list of health-related affinity segments (*e.g.*, food & dining, lifestyles & hobbies, sports & fitness categories). RJN Ex. 5 at 3–4. The categories Plaintiffs list in paragraph 127 are not included in that list. *See id.* Further, Google explains that it "will never use sensitive information like health, race, religion, or sexual orientation to tailor ads to users." *Id.* at 4. Plaintiffs' allegations concerning category (1) are a microcosm of their whole case—vague, confused, and inscrutable assertions generated by flipping through Help Pages, desperately searching for language they can twist into a claim.

As for categories (2) through (4), Plaintiffs' allegations are also based on generic Google Help Pages describing each product, and none of the Help Pages makes any mention of the use of health data in the product or any of its features. SAC ¶¶ 136–44 nn.61–70. The Smart Bidding, placement targeting, Performance Max, and conversion tracking web pages make no mention of the use of health information, analytics data, or ads data from health-related websites. *See id.* For example, Plaintiffs cite a Help Page describing placement targeting, and claim that any ads placed on a health care website must necessarily have been placed by assessing health information previously transmitted through that site. *Id.* ¶ 137 n.62. However, the Help Page makes no reference to health information, and provides no reason to believe that suggested placements based on "past [sic] traffic Google noticed on the site" would mean that (i) the site is transmitting health information; and (ii) Google is using that health information to suggest that placement (as opposed to, *e.g.*, the number of ad placement requests made by the website). In addition, advertisers are prohibited from targeting ads based on health information. *See* Dkt. 158-15; RJN Ex. 9.

Plaintiffs provide one "example" screenshot in paragraph 137 of a Kisqali advertisement that they suggest is a Google Ad. But there is no fact alleged that would indicate the Kisqali ad is a Google Ad, particularly as Mayo Clinic states that, in addition to using Google Ads, the website

also receives advertising inquiries directly.[5] And even assuming the Kisqali ad was placed by Google, no Plaintiff claims that they received the ad, and the SAC does not allege any facts to believe the ad was targeted based on Plaintiffs' interactions with the Websites as opposed to, for example, contextual advertising based on the content of the webpage on which the ad appears.

As another example of their shotgun approach, Plaintiffs quote a sentence from Google's 2022 Form 10-K stating that Google is "investing significantly in areas of health, life sciences, and transportation," and Google receives revenue "from the sale of health technology," to claim that Google "uses Plaintiffs' and Class members' Health Information to inform and develop new services." SAC ¶ 142. Plaintiffs provide no basis to support this inferential leap. This case is not about Google's health-related investments, nor Google's sale of "health technology."

Finally, as for the allegations regarding "personalized content," there are no facts alleged that any Plaintiff received personalized content because they visited one of the Websites. And it is hard to imagine how Plaintiffs could have been damaged by such recommendations, or how the provision of tailored recommendations based on a user's browsing history would constitute a violation of privacy or other laws (indeed, at Google at least, such personalization is gated by an opt-in control, and Plaintiffs do not even allege whether they opted into personalization in the first place). Regardless, the webpages Plaintiffs cite do not support their claim that health information is used to personalize any such recommendations. SAC ¶ 144 n.69.

3. Plaintiffs' allegations defeat the intent element of their claims.

In order to state a claim for violation of Counts 1 through 4 (Wiretap Act, CIPA, invasion of privacy, and intrusion upon seclusion), Plaintiffs must allege intent; that is, that Google acted "purposefully and deliberately and not as a result of accident or mistake," in receiving their personal health information. *See United States v. Christensen*, 828 F.3d 763, 790 (9th Cir. 2015).

Plaintiffs' intent allegations based on Google's terms and policies remain contradictory. As Plaintiffs acknowledge, Google specifically instructs developers not to send personally

[5] *See Advertising and Sponsorship*, MayoClinic.org, https://www.mayoclinic.org/about-this-site/advertising-sponsorship.

identifiable information ("PII") and HIPAA-covered information to Google. SAC ¶¶ 152, 156. And, as Plaintiffs acknowledge, Google prohibits advertisers from targeting ads based on health information. *Id.* ¶ 133. Plaintiffs attempt to minimize these clear prohibitions by arguing that (1) Google's HIPAA policy was not separated into its own webpage until March 2023, and (2) the Google Analytics Terms of Service ("GA TOS") do not expressly reference HIPAA. They reason, baselessly, that Google must have secretly hoped that developers would not find those warnings, or would find them and not understand them, and then willfully violate Google's terms and policies (and their own obligations under HIPAA). *Id.* ¶¶ 151–61. This is several inferential leaps too far. Plaintiffs focus on Google's HIPAA policy from March 2023, perhaps to imply that Google began to warn developers of HIPAA only recently. *See id.* ¶¶ 157, 160, 162–66. Plaintiffs are incorrect, however. That same HIPAA policy has been posted on another webpage since at least 2018. RJN Ex. 4 at 4. The webpage warned developers to "Avoid sending PII to Google when collecting Analytics data," and the HIPAA policy stated, "you may not send Google Analytics encrypted Protected Health Information (as defined under HIPAA), even if it is hashed or salted." *Id.* The policy also stated "Google does not intend uses of Google Analytics to create obligations under [HIPAA] and makes no representations that Google Analytics satisfies HIPAA requirements." *Id.*

Plaintiffs' newfound interpretation of the GA TOS is even less credible. Plaintiffs argue that the TOS' use of the words "You will not" instead of "You may not," somehow turn a developer obligation into a Google promise. SAC ¶ 156 (claiming that the TOS' prohibition "You will not . . . pass information to Google that Google could use or recognize as personally identifiable information" is actually a promise from Google to developers that no PII transmissions will ever occur). This interpretation not only strains credulity, but also ignores the use of "will" in other provisions delineating other actions developers must take. *See, e.g.*, RJN Ex. 1 at 4 ("You . . . will comply with all applicable laws, policies, and regulations"). The GA TOS' requirements that developers "comply with all applicable laws, policies, and regulations relating to the collection of information from Users," "post a Privacy Policy," "provide notice of Your use of cookies, identifiers or mobile devices," "disclose the use of Google Analytics," and obtain user consent

where "obtaining such consent is required by law" apply equally to healthcare providers, and are consistent with Google's HIPAA policy. *Id.* at 4–5.

Next, Plaintiffs claim that because Google intended to market its Ads and Analytics products to the healthcare industry, Google must have intended that healthcare providers use them unlawfully to send Google PHI. SAC ¶¶ 146–50. The basis for this logical leap is a lone document regarding marketing strategies for Google Analytics, in which Google describes its plan to market to the healthcare industry. However, nowhere in the document does Google mention any intent to receive health data, nor an intent that the healthcare industry violate Google's terms of service, policies, and federal law when using the product. Nor do Plaintiffs allege that the use of Google source code is necessarily problematic, nor can they, where they elsewhere acknowledge that HHS guidance provides that "tracking technologies" may be used without violating HIPAA. SAC ¶ 116.

Finally, Plaintiffs argue that if the Websites violated Google's policies by misusing Google's products, Google must have intended for its policies to be violated. SAC ¶ 153. Plaintiffs provide no support for their claim regarding Google's secret intentions. As this Court noted, the only way Google could prevent any risk of collection of health information is by banning healthcare providers from using its products altogether. Dkt. 157 at 8. But there is nothing inherently unlawful about the use of tracking technologies. HHS, and other courts, have recognized their value to healthcare providers. *See* Dkt. 158-6; *Am. Hosp. Ass'n*, 2024 WL 3075865, at *15 (prohibiting hospitals from using analytics would have a "profound chilling effect on providers' use of technology vendors to facilitate critical [unauthenticated public webpages]" and that "it serves nobody to have websites that patients do not know and cannot navigate effectively.").

B. Each of Plaintiffs' claims suffers from more fatal defects.

In addition to the overarching problems discussed above, there are separate, independent reasons to dismiss each of Plaintiffs' claims.

1. Federal Wiretap Act (Count 1)

The Federal Wiretap claim fails because Plaintiffs do not adequately allege intent, as described above. *Supra* Section V.A.3. In addition, the claim fails because the Websites consented

to the use of Google's products by choosing to incorporate the source code on their Websites. *See* SAC ¶ 154 (noting that the "Health Care Provider installs Google Source Code on its web property"); *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021) (no Wiretap violation where "Google's alleged interceptions occurred with the consent of app developers"). Plaintiffs suggest that any Website consent was invalid because (1) "Google obscured and misrepresented the nature of its tracking tools to Health Care Providers"; (2) some Websites issued data breach notices; and (3) the Websites acted with criminal or tortious intent. SAC ¶¶ 221, 223–24. All three of these allegations are unsupported.

First, Plaintiffs' fraud-based allegations fall far short of the heightened pleading requirements of Rule 9(b). *See Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007). Plaintiffs claim that the following documents contain misleading statements: (1) the GA TOS; (2) Google's HIPAA policy; (3) Google's Ad Manager policy; (4) the Google Signals Help Page; and (5) the Universal Analytics IP address Help Page. SAC ¶¶ 145–73. As to the GA TOS and HIPAA policy, they clearly prohibit developers from transmitting PII and personal health information to Google. *Supra* Section V.A.3. The Ad Manager policy similarly states, "publishers must not pass any data to Google that Google could use or recognize as personally identifiable information (PII)." SAC ¶ 158 n.82. Contrary to Plaintiffs' assertions, these prohibitions clearly describe *developer* obligations, and not Google promises. It defies credulity to interpret these prohibitions instead as promises that Google does not receive PII regardless of what developers choose to send. As to Google Signals, Plaintiffs vaguely claim that "Google assured Health Care Providers using Google Signals that it had user consent to do so, but Google did not obtain user consent for collection of Health Information." SAC ¶ 223(b). Plaintiffs' discussion about Signals is sparse, but appears to hinge upon a Help Page describing the feature. *Id.* ¶ 105. The Help Page states, when a developer activates Signals, "Google Analytics collects additional information about users who have consented to Ads Personalization." RJN Ex. 8 at 1. Plaintiffs do not allege any facts to support their contention that Google took actions in contradiction of its Help Page and collected such information without user consent. Finally, Plaintiffs claim that the "IP address masking" feature

in Universal Analytics is misleading because the Help Page claims that IP addresses will not be stored, but in reality the addresses are stored in a "fuzzified" manner. SAC ¶ 159. Plaintiffs mistakenly conflate two different features: (i) the "IP address masking" feature in Universal Analytics (the older version of Google Analytics); and (ii) the dropping of IP address entirely in Google Analytics 4. In Universal Analytics, developers could choose to "mask" IP addresses by truncating the address. RJN Ex. 7 at 1. In Google Analytics 4, IP addresses are not "masked," but rather are no longer stored in their entirety. *Id.* ("In Google Analytics 4, IP masking is not necessary since IP addresses are not logged or stored.").

Second, Plaintiffs claim that any website consent is invalid because some healthcare providers have issued notices regarding potential data breaches, attaching three health breach notifications as exhibits. SAC ¶ 223. To begin with, only one of the notices was issued by one of the Websites. Dkts. 158-3, 158-12, 158-13. The notices also do not identify any fraudulent conduct, false promises, or misleading representations by Google, nor claim that the healthcare provider was under any false impressions about the Google source code. *See id.* And the notices don't identify the specific data that were actually transmitted to Google, stating, for example, that certain tracking tools (including tools by Google, Bing, X (Twitter), and Meta) "*may*" have transmitted certain types of information to those vendors.[6] *See, e.g.*, Dkt. 158-3 at 2; Dkt. 158-12 at 3 (listing types of information that "may have been shared"); Dkt. 158-13 at 3 (same).

Finally, Plaintiffs claim that any consent is invalid because the healthcare providers would have only provided that consent for a criminal, tortious, and unlawful purpose. SAC ¶ 224. Plaintiffs cannot have it both ways. On the one hand, Plaintiffs claim that any consent obtained was invalid because the healthcare providers were misled by Google's representations regarding the functionality of its products. *See, e.g.*, SAC ¶¶ 159–60, 223. On the other hand, Plaintiffs claim that the healthcare providers knowingly and intentionally provided consent in order to commit

[6] The fact that a HIPAA-covered entity has issued a breach notification does not necessarily mean that the entity has determined there is a high risk that PHI has been compromised. *See Breach Notification Rule*, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

torts, crimes, and violations of the law. *See id.* ¶ 224.[7] Regardless, either allegation fails. The crime-tort exception to the Wiretap Act requires that the "communication [be] intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). The crime-tort exception asks what the *interceptor's* purpose was in conducting the interception, not a party's purpose for consenting to the interception. In this lawsuit, Plaintiffs are claiming that *Google*, not the Websites, was the interceptor. And Google's purpose in offering Ads and Analytics products, as this Court noted, "has plainly not been to perpetuate torts on millions of Internet users, but to make money." Dkt. 157 at 11 n.4 (quotation omitted). And even if the crime-tort exception applied to the Websites, there is no reason to believe that the Websites used Google source code to commit a crime or tort, as opposed to trying to understand how visitors are using their websites. *See, e.g.*, *Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *10 (finding no crime-tort exception where Kaiser collected plaintiffs' information for market research and consumer analysis, rather than to commit a crime or tort); Dkt. 158-3 at 2 (Kaiser explaining that tracking technologies are used "to understand how consumers interact with websites and mobile applications"); Dkt. 158-12 at 2 (Advocate Aurora Health "uses third-party vendors to evaluate the trends and preferences of patients as they use the health system's websites"); Dkt. 158-13 at 3 (Allina Health "has no evidence that Google used this data for any purpose other than providing analytic services to Allina Health"). And besides, Plaintiffs do not allege that they received any targeted advertisements based on their health information. *Cf. Kurowski v. Rush Sys. for Health*, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2003) (finding the crime-or-tort exception applied where plaintiff alleged she was targeted with "particular advertising associated with her particular health conditions").

2. California Invasion of Privacy Act (Count 2)

Plaintiffs allege violations of Sections 631 and 632 of CIPA. Section 631 prohibits wiretapping, making it unlawful to "intentionally intercept the content of a communication . . . or

[7] As noted previously, Plaintiffs' counsel have squarely placed the blame upon healthcare providers in a plethora of other cases in which only the healthcare provider has been named as a defendant. *Supra* Section III.A.

to [willfully] read, attempt to read, or learn the 'contents or meaning of any message, report, or communication while the same is in transit . . . ' without the consent of all parties to the communication." *Rodriguez*, 2021 WL 2026726, at *6 (quotation omitted). Section 632 of CIPA prohibits eavesdropping, *i.e.*, "record[ing] [a] confidential communication" "intentionally and without the consent of all parties" to the communication. Cal. Penal Code § 632. As an initial matter, both CIPA claims fail because Plaintiffs fail to allege that Google acted willfully or with intent to intercept, read, or record Plaintiffs' confidential health communications. *Supra* Section V.A.3. Both claims additionally fail for the reasons described below.

Section 631: Plaintiffs have alleged facts sufficient to establish only that Google acted as an extension of the Websites, processing their data only as instructed by the Websites. *See Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021). Recently, Judge Chen held that whether a third-party vendor functioned as a mere extension of the website turned on whether the vendor was "subject to the control" of the website. *Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *17. As is apparent in the SAC, the Websites are able to control whether and how Google processes their data by choosing whether to install the source code, choosing what pages on which to install the source code, and choosing what features and settings to enable or disable. *See, e.g.*, SAC ¶¶ 105, 135, 154. Whether and how Google processed the Websites' data is "subject to [the Websites'] control and ability to limit the use of dissemination of the medical data"; therefore, Google cannot be held liable when all that it did was "collect and/or use information for [the Websites'] benefit only," and not for its own benefit "(*e.g.*, to sell to others)." *Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *18.

Plaintiffs' own exhibits show that Kaiser and two other healthcare providers described their relationship with Google Analytics as a mere third-party vendor. Kaiser states that they may have used Google Analytics to "understand how consumers interact with websites and mobile applications," and does not state that Google Analytics data was used to advertise or for any other purpose. Dkt. 158-3 at 2. The article describing Allina Health states that Allina Health "has no

evidence that Google used this data for any purpose other than providing analytic services to Allina Health." Dkt. 158-13 at 3. And the article describing Advocate Aurora Health states that the website was using third-party vendors "to evaluate the trends and preferences of patients as they use the health system's websites," and makes no mention of use of the data for advertising or other purposes. Dkt. 158-12 at 2. A third-party vendor cannot violate Section 631 when the vendor merely "provides a software service that captures its clients' data, hosts it on the [vendor's] servers, and allows the clients to analyze their data." *Noom*, 533 F. Supp. 3d at 832. And while Plaintiffs claim that Google, in general, uses ads and analytics data for advertising and "personalized" recommendations, Plaintiffs do not provide any facts to support their allegations that Google's general product descriptions apply in the same manner to data received from health-related websites, particularly where Google's policies and terms specifically provide otherwise. *Supra* Section V.A.1; Ex. 158-15; Ex. 158-14. And much advertising is also a mere vendor activity, *e.g.*, placing ads on specified websites as directed by the advertiser.

Finally, Plaintiffs' allegations do not establish that the data transmitted to Google constituted the "content" of a communication. The data Plaintiffs allege was transmitted to Google consists of URLs, HTTP request headers, browser cookies, IP addresses, user agents, and device properties. These types of data constitute record information, not content, under Section 631. *See John Doe v. Cedars-Sinai*, 2024 WL 3303516, at *2 (Cal. Super. Ct. June 5, 2024) (holding that IP addresses, pages the patient clicked on, and doctor's names did not constitute "contents of a communication" under Section 631); *see also Jones v. Peloton Interactive, Inc.*, 2024 WL 1123237, at *4 (S.D. Cal. Mar. 12, 2024) (holding that "IP address, device used to connect to website, web browser used, date and time of communication, words used to prompt the chat" was "record" information, not content); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) (HTTP referrer information was not "contents" of a communication under the Wiretap Act); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 935 (N.D. Cal. 2015) (user's identification information and record of browsing history were not "content").

Section 632: The Section 632 claim fails because Google did not "record" the data transmitted; rather, the Websites recorded the data. The Websites chose what data to record and transmit to Google, whether to place the Google source code on their webpages, and which pages to place the code on. After placing the source code, the Websites chose what data to record, what custom events to create (if any), and what optional features to enable or disable.

Plaintiffs also have not shown that Google recorded their "confidential communications." As discussed, Google instructed the Websites to disclose the use of Google Analytics, post a privacy policy, and obtain consent where required by law. *See* RJN Ex. 1 at 4–5. Plaintiffs do not have a reasonable expectation of privacy in their analytics data where the Websites disclosed their use of Google Analytics. Plaintiffs' exhibits do not show any of their "confidential communications" either. The "sample" data in Exhibits 1 and 2 do not contain messages with healthcare providers, diagnoses, or confidential information in which a consumer might have a reasonable expectation of privacy. *See* Dkts. 158-1, 158-2; *Cedars-Sinai*, 2024 WL 3303516, at *4 ("IP addresses, webpages, and doctors' names are not confidential communications.").

3. Constitutional / Common Law Privacy (Counts 3 and 4)

To state a claim for common law intrusion upon seclusion or invasion of privacy under the California Constitution, a plaintiff must plead that (1) "the defendant [] intentionally intrude[d] into a place, conversation, or matter, as to which the plaintiff has a reasonable expectation of privacy," and (2) "the intrusion [] occur[ed] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 286 (2009); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020).

First, Plaintiffs' allegations do not support that Google had the intent to intrude into a conversation or matter in which the Plaintiffs had a reasonable expectation of privacy. As discussed, the GA TOS and policies requiring the Websites to disclose the use of Google Analytics and refrain from collecting PII and personal health information undermine Plaintiffs' claims that Google "intended" to receive their health information in violation of their privacy. *Supra* Section

V.A.3; *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016) (plaintiff failed to plead intent where the allegations contradicted Facebook's Terms of Service).

Second, Plaintiffs cannot establish that they had a reasonable expectation of privacy in the data that was transmitted. Even assuming the types of data in Exhibits 1 and 2 are representative of what would have been transmitted for Plaintiffs, that type of "metadata" information does not rise to the level of PHI because the metadata does not reveal a patient's diagnosis or treatment information. Based on the metadata, one cannot discern *why* a visitor accessed a webpage about Type 2 diabetes—*i.e.*, whether the visitor was curious about the condition, accidentally navigated to the page, or was diagnosed with Type 2 diabetes. *See Am. Hosp. Ass'n*, 2024 WL 3075865, at *15 ("metadata shared with third-party vendors can only reveal sensitive PHI if an unknown subjective intent is communicated."). "Without knowing information that's never received—i.e., the visitor's subjective motive—the resulting metadata could never identify that individual's PHI." *Id.* at *14. The Ninth Circuit similarly stated that data showing only that "Plaintiffs searched and viewed publicly available health information . . . cannot, in and of itself, reveal details of an individual's health status or medical history," and is not "qualitatively different" or more "sensitive" than other web-browsing data. *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018); *see also Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 945–55 (N.D. Cal. 2017) ("browser settings, language, operating system, IP address, and the contents of cookies" and the URLs for pages "containing information about treatment options for melanoma, information about a specific doctor, [or] search results related to the phrase 'intestine transplant'" do not constitute PHI); *Cousin v. Sharp Healthcare*, 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023) (data about plaintiffs' use of the "website to 'research . . . doctors,' 'look for providers,' and 'search for medical specialists'" was not PHI because "'nothing about [the] information relates specifically to plaintiffs' health'"); *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosure of device identifier, personal data, and geolocation information "does not constitute an egregious breach of social norms").

Finally, Plaintiffs cannot establish that the intrusion occurred in a highly offensive manner. The SAC establishes only that Google Analytics or Ads cookies were present on certain URLs, but does not differentiate between authenticated and unauthenticated webpages. And, given that Google required the Websites to disclose their use of Google Analytics, any collection and transmission of data to Google would not be "highly offensive." As HHS acknowledges, tracking technologies are commonly used to "collect and analyze information about how users interact with regulated entities' websites or mobile applications." RJN Ex. 10 at 2. Plaintiffs do not allege that they received any advertisements or personalized recommendations that might suggest Google utilized their data in the manner they claim. Even use of tracking technologies on authenticated webpages is not a *prima facie* invasion of privacy. Tracking technologies may be placed on user-authenticated webpages, but must be utilized in compliance with HIPAA. *See id.* HHS notes that information regarding an individual's diagnosis, treatment, prescription information, and appointments they've made may disclose PHI, but Plaintiffs' "sample" transmissions do not even contain such information. *See* Dkt. Nos. 158-1, 158-2. Finally, Plaintiffs' allegations do not show that Google collected or used the information for its own purposes, or "materially increase[d] the risk of the dissemination of the collected information." *Kaiser Found. Health Plan, Inc*, 2024 WL 1589982, at *19 (holding that the intrusion was not highly offensive where "Kaiser simply hired a third party to do work for Kaiser's own benefit").

4. Breach of Contract (Count 5)

Plaintiffs bring the breach of contract claim on behalf of Google account holders only, and as to Google's Terms of Service and Privacy Policy. SAC ¶¶ 275–92.

Promise 1: Plaintiffs claim that Google breached the Privacy Policy's promise to refrain from collecting Health Information. "Health Information" is defined in the Privacy Policy as "medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app." Dkt. 158-14 at 19. To begin with, this provision does not apply to Plaintiffs, as Plaintiffs do not allege they used "Google

services that offer health-related features." *Id.* In addition, Plaintiffs do not claim that Google collected their medical history, vital signs, or health metrics. Even assuming Google received data similar to that in Exhibits 1 and 2 to the SAC, the data, at most, consist of pseudonymous URL metadata, and do not contain "Health Information" as defined by the Privacy Policy; that is, medical history, vital signs, or health metrics (or similar information) about an identifiable person. *See, e.g.*, *Kurowski v. Rush Sys. for Health*, 2024 WL 3455020, at *2 (N.D. Ill. July 18, 2024) ("IP addresses, cookie identifiers, device identifiers, account numbers, URLs, and browser fingerprints" are "just metadata" and do not constitute IIHI under HIPAA). Exhibits 1 and 2 do not show the substance of Plaintiffs' private communications related to their care or any particular health or treatment information. *See id.*; *see also Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836, 843 (N.D. Ill. 2023) (same); *Hartley v. Univ. of Chicago Med. Ctr.*, 2023 WL 7386060, at *2 (N.D. Ill. Nov. 8, 2023) (IP addresses, Facebook IDs, cookie identifiers, device identifiers, account numbers, URLs, and buttons, pages, and tabs that were clicked and viewed do not constitute IIHI under HIPAA). Rather, the data contained in Plaintiffs' exhibits consist of only "Internet, network, and other activity information," which Google discloses as a category of information it collects under Privacy Policy. *See* Dkt. 158-14 at 17. Like in *Smith v. Facebook, Inc.*, "[t]he data show only that Plaintiffs searched and viewed publicly available health information that cannot, in and of itself, reveal details of an individual's health status or medical history," and therefore consists of only "Internet, network, and other activity information.". *See* 745 F. App'x at 8–9; *see Hammerling v. Google LLC*, 2024 WL 937247, at *2 (9th Cir. Mar. 5, 2024) (affirming dismissal of fraud, breach of contract, invasion of privacy, and intrusion upon seclusion claims where Google's privacy policy "unambiguously discloses Google's collection of user activity data in third-party apps").

Promise 2: Plaintiffs claim that Google breached the Privacy Policy's promise not to use health information for personalized advertising by using "use[s] Health Information in advertising products and services that are personalized," such as placement targeting, artificial intelligence, developing new services, and personalized recommendations. *Id.* ¶¶ 287, 291. As previously

discussed, Plaintiffs' fraud-based allegations that Google engages in such conduct despite promising otherwise are vague, unsupported, and fall far short of the standard required by Rule 9(b). *Supra* Section V.A.1. Plaintiffs also do not allege they received any targeted advertisements or personalized recommendations based on their interactions with the Websites. The documents that Plaintiffs rely upon for these allegations do not mention health information, but are simply disclosures and Help Pages that describe how Google's products work in general.[8]

Finally, not only are Plaintiffs unable to allege that Google breached any of these promises, they also cannot show that the purported breach caused them any damage. *See In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019). Plaintiffs' allegations do not support that their health information was transmitted to Google. *Supra* Section V.A.1. Plaintiffs also do not allege they received any targeted advertisements based on their health information. And Plaintiffs do not allege Google shared their health information with third parties. *Cf. In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F .Supp. 3d 767, 776, 784, 802 (N.D. Cal. 2019) (alleging Facebook shared its users' personal information with third parties).

5. Breach of Implied Covenant for Good Faith / Fair Dealing (Count 6)

The SAC fails to allege facts showing that Google acted to "injure the right[s] of [Plaintiffs] to receive the benefits of [any] agreement," as required for breach of the implied covenant. *See Careau & Co. v. Sec. Pac. Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1393 (1990). The Court previously held that Plaintiffs "failed to state a claim for breach of the implied covenant" since they "have not adequately alleged that Google's interpretation of 'health information' or 'personally identifiable information' is objectively unreasonable." Dkt. 157 at 20. Plaintiffs' claim, as amended, is unchanged; the deficiencies the Court identified have not been corrected. *Id.*

The SAC contains no new allegations regarding Google's interpretation of "Health Information." There still is no plain statement of how Google allegedly "abused its power to

[8] Though Plaintiffs allege that advertisers were allowed to violate Google's advertising policy, *see* SAC ¶ 135 n.57, Plaintiffs base their breach-of-contract claim upon only *Google's* alleged collection and use of health information, not the Websites' collection or use. SAC ¶¶ 285, 291.

define" this term or made any "effort to limit [its] meaning." SAC ¶¶ 296–97. Nor is there any plain statement of how Google allegedly made an "effort to change the meaning of the term 'identifiable'" or "to interpret 'personalized advertising'" in an objectively unreasonable way, much less how any such "effort" would be an abuse of power to define contractual terms. *See id.*

The SAC's allegations regarding the implied-covenant claim do not even specify which "terms of the contract" Google abused its power to define. *See id.* These allegations specifically reference "Health Information"—so capitalized. *Id.* But this is Plaintiffs' own defined term in the SAC (*see* SAC ¶ 21); it is *not* the alleged contractual terms "health information" or "Health information" that Plaintiffs reference in their breach-of-contract claim (*see* SAC ¶¶ 181, 285). Plaintiffs' implied-covenant claim thus rests partly on the nonsensical allegation that Google made some unspecified "effort to limit the meaning of" *Plaintiffs' defined term*. This is incoherent. Such allegations fail to satisfy basic pleading standards, including Rule 8(a)(2)'s requirement of a plain statement—especially in the context of a twice-amended complaint.

6. Unjust Enrichment (Count 7)

In its Order, the Court dismissed Plaintiffs' claim for unjust enrichment "because the plaintiffs have not stated a claim against Google for any unlawful conduct." Dkt. 157 at 20. The SAC does not add any allegations related to this claim—it only replaces the allegation that Google engaged in the "sale" of Plaintiffs' information with the more anodyne allegation that Google engaged in the "use" of their information (see SAC ¶ 306)—so it fails again here. This claim also fails because unjust enrichment is not an independent cause of action where, as here, a valid contract is alleged to cover the subject matter at issue. *See Saroya v. Univ. of the Pac.,* 503 F. Supp. 3d 986, 998 (N.D. Cal. 2020).

VI. CONCLUSION

In its Order Granting Motion to Dismiss, the Court stated "[t]he Court is increasingly skeptical, based on what's transpired in the case so far, that the plaintiffs can successfully amend their complaint." Dkt. 157 at 2. Plaintiffs' SAC shows that the Court's skepticism was well-founded. Google respectfully requests that the Court dismiss the SAC with prejudice.

Dated: September 3, 2024

WILLKIE FARR & GALLAGHER LLP
Benedict Hur
Simona Agnolucci
Eduardo Santacana
Joshua Anderson
David Doak
Tiffany Lin
Naiara Toker
Nadim Houssain
Harris Mateen

By: */s/ Benedict Hur*
Benedict Hur

Attorneys for Defendant
GOOGLE LLC